SYSTEM AND METHOD FOR EFFICIENT AND SECURE REVOCATION OF A SIGNATURE CERTIFICATE IN A PUBLIC KEY INFRASTRUCTURE

ABSTRACT

System and method for revocation of a signature certificate in a Public Key Infrastructure (PKI) that includes an enterprise with one or more servers, a directory, a registration web server, and one or more client platforms that allow users to access the servers of the enterprise. A user may desire to revoke a potentially compromised signature certificate of the user, or a manger of the user may revoke a signature certificate because it has been lost by the user, or the manager no longer desires that the user has access to servers of an enterprise. A user or personal revocation authority (manager) initiates a revocation process by creating an authenticated secure channel with a registration web server. Using the authenticated secure channel, the user or personal revocation authority requests the registration web server revoke a user signature certificate. The registration web server queries a directory to verify that the personal revocation authority is permitted to revoke the signature certificate of the user. The user signature certificate is revoked. The directory is notified by the registration web server of revocation of the user signature certificate. A user entry in the directory is set to a state without a signature certificate. A process for a new signature certificate for the user may now occur.